PATENT
Attorney Docket No. 028572-003200US
Client Ref. No. VRSN 0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No. 7016
Nicolas Popp et al.	Examiner: James D. Nigh
Application No.: 10/590,415	Technology Center/Art Unit: 3685
Filed: October 20, 2006	APPELLANTS' BRIEF UNDER 37 CFR §41.37
For: TOKEN AUTHENTICATION SYSTEM AND METHOD	

Mail Stop Appeal Brief
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

Further to the Notice of Appeal mailed on July 13, 2010 for the above-referenced application, Appellants submit this Brief on Appeal. This Brief is timely filed due to the constructive petition for extension of time submitted herewith. The Commissioner is authorized to charge any fees due, including the fee for this brief, or to credit any overpayment to the Deposit Account of Townsend and Townsend and Crew LLP, Deposit Account No. 20-1430.

1. REAL PARTY IN INTEREST

The real party in interest is Symantec Corporation.

2. RELATED APPEALS AND INTERFERENCES

None.

3. STATUS OF CLAIMS

Claims 1-11 are pending and are the subject of this appeal.

4. STATUS OF AMENDMENTS

No amendments have been filed after the Final Office Action mailed April 13, 2010.

5. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 recites a method for calculating a One Time Password, comprising: concatenating, by a computer, a secret with a count, where the secret is uniquely assigned to a token and is shared between the token and an authentication server, and the count is a number that increases monotonically at the token with the number of One Time Passwords generated by the token and increases monotonically at the authentication server with each calculation by the authentication server of a One Time Password (p. 3, lines 16-32; p. 4:30-5:11; :Figs. 1-2:110); calculating, by a computer, a hash based upon the concatenated secret and count (p. 3, lines 16-32; p. 4:30-5:11; :Figs. 1-2:110); and truncating the result of the hash to obtain a One Time Password (p. 3, lines 16-32; p. 4:30-5:11; :Figs. 1-2:110).

Independent claim 2 recites a method for authenticating a request for access to a resource, comprising: receiving by an authentication server a request for authentication that includes a serial number that is uniquely associated with a token, a personal identification number

associated with a user and a One Time Password generated by a token, wherein the One Time Password is based upon the value of a count at the token and a secret shared between the token and the authentication server (p. 3, lines 16-32; p. 4:30-5:11; p. 9:30-10:6; p. 10:15-18; Fig. 1); retrieving by the authentication server the value of a count that corresponds to the token based upon the serial number (p. 10:20-24; Fig. 1); retrieving by the authentication server the secret that corresponds to the token based upon the serial number (p. 10:20-24; Fig. 1); calculating by the authentication server the value of a One Time Password based upon retrieved values of the count and the secret corresponding to the token (p. 10:24-26; Fig. 1); comparing the calculated One Time Password with the received One Time Password (p. 10:24-26; Fig. 1); and if the calculated One Time Password corresponds to the received One Time Password, the request is determined to be authenticated (p. 10:26-27; p. 11:6-9; Fig. 1); if the calculated One Time Password does not correspond to the received One Time Password, then incrementing the value of the count at the authentication server and recalculating the One Time Password based upon the incremented count and the secret, and comparing the recalculated One Time Password with the received One Time Password (p. 10:28-11:6; Fig. 1); if the recalculated One Time Password does not correspond to the received One Time Password, then repeating to increment the count and to recalculate the One Time Password until the recalculated One Time Password corresponds to the received One Time Password (p. 10:28-11:6; Fig. 1).

Independent claim 6 recites a method for authenticating a request for access to a resource, comprising: receiving by an authentication server a request for authentication that includes a username that is uniquely associated with a user, a personal identification number associated with a user and a One Time Password generated at a token, wherein the One Time Password is based upon the value of a count at the token and a secret shared between the token and the authentication server (p. 3, lines 16-32; p. 4:30-5:11; p.9:24-28; p. 9:30-10:6; p. 10:15-18; p. 11:12-27; Figs. 1-2); retrieving by the authentication server the value of a count that corresponds to the token based upon the username (p. 10:20-24; Fig. 1); retrieving by the authentication server the secret that corresponds to the token based upon the username (p. 10:20-24; Figs. 1-2); calculating by the authentication server the value of a One Time Password based upon retrieved

values of the count and the secret corresponding to the token (p. 10:24-26; Figs. 1-2); comparing the calculated One Time Password with the received One Time Password (p. 10:24-26; Figs. 1-2); and if the calculated One Time Password corresponds to the received One Time Password, the request is determined to be authenticated (p. 10:26-27; p. 11:6-9; Figs. 1-2); if the calculated One Time Password does not correspond to the received One Time Password, then incrementing the value of the count at the authentication server and recalculating the One Time Password based upon the incremented count and the secret, and comparing the recalculated One Time Password with the received One Time Password (p. 10:28-11:6; Figs. 1-2); if the recalculated One Time Password does not correspond to the received One Time Password, then repeating to increment the count and to recalculate the One Time Password until the recalculated One Time Password corresponds to the received One Time Password (p. 10:28-11:6; Figs. 1-2).

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-11 stand rejected under 35 U.S.C. §103 as unpatentable over Matyas (U.S. Patent No. 5,953,420) in view of Newcombe (U.S. Pub. No. 2003/0172269).

7. ARGUMENT

Many of the issues in this appeal relate to whether the claim term "token" has been given an appropriate interpretation by the Office during prosecution. The Examiner has applied an interpretation that renders the term equivalent to a mere data structure, specifically a Kerberos authentication "ticket" described in one of the cited references. In contrast, Appelants maintain that a proper interpretation of the term must be consistent with the use of the term in the claims themselves and with the use of the term in the specification. The claims require the recited "token" to be capable of performing operations, such as generating one time passwords, that simply cannot be performed by mere data structures such as the tickets cited by the Examiner. The Examiner has attempted to remedy this deficiency by focusing on whether the specification requires the recited token to be a purely physical device, and by improperly reading the token functionality out of the claims. As explained in further detail below, the Examiner's position is

improper and is insufficient to remedy the clear deficiencies of the cited art, and the rejections should be reversed.

Claims 1-11: The Cited References Do Not Disclose The Recited "Token."

To support a prima facie case of obviousness, the Examiner must demonstrate that each feature recited in the claims is found in the cited art, or provide explicit reasoning to support the finding that the features would be obvious to one of skill in the art at the time the invention was made. See M.P.E.P. §§ 2141, 2142. The Office Action asserts that each and every feature recited in the claim is shown by the cited references. Thus, to support the rejection of these claims, the Examiner must show where each feature recited in the claim is disclosed by one of the cited references.

The Final Office Action Fails to Show that the Cited References Disclose or Suggest a "Token."

Claim 1 recites, in relevant part:

> A method for calculating a One Time Password, comprising:
>
> where the secret is uniquely assigned to a token and is shared between the token and an authentication server; and
>
> the count is a number that increases monotonically at the token with the number of One Time Passwords generated by the token and increases monotonically at the authentication server with each calculation at the authentication server of a One Time Password;

Independent claims 2 and 6 also recite a token that generates One Time Passwords. The Office Action admits that "Matyas does not explicitly disclose a token," but asserts that "Newcombe teaches a token and a method of assigning a secret to a ticket (similar to a token)." Office Action, p. 4 (emphasis added). Appellants respectfully disagree.

A "ticket" is not "similar to a token" as that term would be understood by one of ordinary skill in the art. A ticket is a mere passive data structure that is produced by another device (such

as an authentication server). Once the ticket is produced, no further changes are made to that particular ticket. A token, on the other hand, is capable of performing some functionality including creating and sending data structures, such as a One Time Password and/or the type of information that is carried on a ticket as disclosed by Newcombe, that can be used to authenticate a user. Indeed, insofar as they may be used for similar purposes, a ticket is more like the data sent by the token rather than the token itself. The use of tokens is described at page 1, line 30 – page 2, line 10, page 2, lines 22-26, and throughout the specification as filed. Based on the present disclosure, the explicit requirements of the claim language, and the use of the term in the art, a person of ordinary skill in the art would not consider a ticket to be equivalent to a token as recited in the claims.

Furthermore, even if the term "token" could be considered to include a "ticket," the tickets recited in Newcombe do not – and cannot – perform the functions of a token as recited in the claims. Newcombe is directed to an improved system and method for authenticating a client in a distributed environment using Kerberos-style authenticators. Newcombe, Abstract; ¶ 0002. Newcombe involves the use of three different types of servers: an Authentication Server, a Ticket-Granting-Server, and Content Servers. *Id.* at ¶¶ 0064, 68. The Authentication Server, after it authenticates a client, issues a ticket-granting-ticket, which usually contains a server readable portion (i.e. encrypted so that only the Ticket-Granting-Server can read), a client readable portion (usually encrypted with the clients hash salted password), and a modified authenticator (including a timestamp, local IP address, and remote IP address). *Id.* at ¶ 0064-65. The ticket-granting-ticket is then delivered to the Ticket-Granting-Server, which utilizes the server readable portion of the ticket-granting-ticket (along with other information) to authenticate the user. *Id.* at ¶ 0068. The ticket granting server then gives the client content tickets that permit the client to access the Content Servers. *Id.* at ¶ 0072. The Content Servers utilize the content tickets (along with other parameters) to authenticate the user and allow access to the specific content. *Id.*

The tickets described in Newcombe are simply messages containing encrypted information that are delivered to a client by either the Authentication Server or the Ticket-Granting-Server. Newcombe, ¶¶ 0064-65, 68. There is no disclosure that suggests that any of

these "tickets" are capable of generating anything, let alone that a one time password is generated by the "ticket." Indeed, the ticket is already in its final form when the client receives it, and the ticket itself is passed along to the appropriate server to authenticate the client; the client cannot modify the server readable portion of any ticket because it is encrypted. *Id.* at ¶ 0065 ("tamper-proof server readable portion"); ¶ 0032 (describing how a ticket can be encrypted to protect the information on it). For at least this reason, a person of ordinary skill in the art would not interpret Newcombe's "tickets" to disclose the use of a token that generates One Time Passwords as recited in claim 1.

This is further evidenced by Newcombe itself, which explicitly addresses tokens and the use of tokens in authentication systems:

> Once the software is downloaded, the user may share the downloaded software with a friend. Some Internet sites attempt to limit sharing of the software by requiring a user password, a Compact Disc (CD) key, token, or the like to be provided to the Internet server prior to obtaining access to the software. Typically, should a password, token, or key be shared or stolen, the unauthorized user would still be able to access the software. Therefore, there is a need in the industry for enabling improved authentication in a distributed environment. Thus, it is with respect to these considerations and others that the present invention has been made.

Newcombe, ¶ 0004. Newcombe thus distinguishes between a "token" and the "tickets" cited by the Office Action, and indicates that the two are not equivalent. In fact, Newcombe states that a problem with using tokens is that if the token gets lost or stolen then an unauthorized individual could have continued access to the protected content. Therefore, it is not reasonable to suggest that the tickets described in Newcombe's system are similar to a token, as that term would be understood to one of ordinary skill in the art, when the alleged limitations of using tokens were one of the stated reasons that Newcombe implemented a system that utilizes tickets instead of relying on tokens, passwords, or other similar techniques.

The Final Office Action's "Broadest Reasonable Interpretation" is Inconsistent with the Present Disclosure and with the Use of Terms in the Claims.

When interpreting a claim term, the "broadest reasonable interpretation" applied by the Office must be consistent with the use of the term in the specification. M.P.E.P. §2111. The present specification indicates that "tokens" are understood in the art to be devices used for authentication:

> A token is a device that can be used to authenticate a user. It can include one or more secrets, some of which can be shared with a validation center. For example, a token can store a secret key that can be used as the basis for calculating a One Time Password (OTP). A OTP can be a number (or alphanumeric string) that is generated once and then is not reused. The token can generate an OTP and send it along with a unique token serial number to an authentication server. . . . To further strengthen the link from the user to the token, the user can establish a Personal Identification Number (PIN) shared with the token that must be entered by the user to unlock the token. Alternatively, the PIN can be shared between the user, the token and the authentication server, and can be used with other factors to generate the OTP. A token typically implements tamper-resistant measures to protect the secrets from unauthorized disclosure.

¶ 0004. The use and configuration of tokens in the present invention is further described throughout the specification, and these features are provided only as non-limiting illustrations. Newcombe's tickets cannot properly be said to have any of these properties – they are mere data structures (*see* paragraph 0007 of Newcombe), and they are not capable of generating an OTP, being locked or unlocked with a PIN, or having tamper-proof measures that prevent disclosure of information contained within them. For at least this reason, the interpretation applied by the Office Action to the tickets in Newcombe is inconsistent with the use of the claim terms in the specification.

The Arguments Presented in the Final Office Action Do Not Remedy the Defects of Newcombe as Applied.

The Final Office Action attempts to rebut the points presented above using several arguments. First, the Examiner presents definitions of the term "token" taken from the Microsoft Computer Dictionary. One definition refers to a "token ring network," in which a "token" data structure is passed from node to node. A second definition refers to a "token" in parsed data, such as a variable name or reserved word. The Final Office Action argues that this is the

"traditional definition" of the term "token," (*see* Final Office Action, p. 3-4), and seems to suggest that the definition demonstrates that Newcombe's "ticket" is equivalent to the claimed "token."

This argument merely shows that the term "token" may have many different meanings in the art. However, any interpretation given to claim terms must be consistent with the use of the term in the specification and claims. *See* M.P.E.P. §2111. A "token," as used throughout the present application including the claim language, must be capable of generating a One Time Password. In fact, the Final Office Action even cites a portion of the specification that indicates that in the present invention One Time Passwords "are generated by a token." (Final Office Action, p. 3, line 17-18.) The "tokens" mentioned in the reference cited by the Final Office Action, as with those in Newcombe, are mere data structures that cannot generate a One Time Password. The definitions provided in the Final Office Action are examples of other uses of the term "token" that are inconsistent with the use of the term in the present application and, therefore, cannot serve as the basis of a proper interpretation of this term during prosecution.

The Examiner next argues that the functional requirements of the recited "token" in the claims and the specification do not "manipulatively affect the method" (p. 4, lines 3-8) and that any such requirements represent "simply non-functional descriptive material" that is not entitled to patentable weight (p. 5, lines 4-11). This is incorrect.

The claims are directed to techniques for generating One Time Passwords using information from a token. For example, claim 1 recites such a method that comprises concatenating a secret with a count. Notably, the recited "count" refers to "a number that increases monotonically at the token with the number of One Time Passwords generated by the token." Each feature recited in claim 1 uses the "count" directly or indirectly. Thus, the fact that the token is capable of generating One Time Passwords is not merely non-functional descriptive material, as alleged in the Final Office Action; rather, it is a feature that affects the functionality and results of the claimed method that must be given patentable weight.

Finally, the Final Office Action argues that Matyas discloses "workstations" and Newcombe discloses a server and a client device, all of which are physical devices. Although not stated explicitly, the Final Office Action seems to suggest that these devices provide further

disclosure of a physical "token." However, the Office Action does not allege that these devices correspond to the recited "token," nor is there any evidence or argument to show that they perform the functions recited in the claims and disclosed in the present specification. Therefore, the mere fact that the references disclose physical devices is insufficient to remedy the defects of the rejection addressed above.

For at least these reasons, the Final Office Action and the art as applied fail to support a *prima facie* case of obviousness of independent claims 1, 2 and 6. The rejection of dependent claims 3-5 and 7-9 is similarly unsupported, and these claims are allowable for at least the same reasons as the independent claims. For at least this reason, the rejection of claims 1-11 should be reversed.

Claims 1-11: The Office Action Fails to Show that the Cited References Disclose or Suggest a Secret that is Uniquely Assigned to a Token.

Claim 1 recites, in relevant part:

> A method for calculating a One Time Password, comprising:
>
> where the secret is uniquely assigned to a token and is shared between the token and an authentication server; and

Claims 10 and 11 recite similar features The Final Office Action admits that Matyas does not disclose, "where the secret is uniquely assigned to [a] token and is shared between the token and an authentication server," but asserts that Newcombe teaches, "a method of assigning a secret to a ticket (similar to a token). Office Action, p. 4. Appellants respectfully disagree.

Even assuming, *arguendo*, that a ticket in Newcombe and a token as recited in the claims are similar, Newcombe does not teach that the secret is uniquely assigned to a "ticket." (interpreted as the recited "token"). Appellant notes that the Final Office Action does not specifically mention what it considers to be the secret that is "uniquely assigned" to the ticket in Newcombe. However there is simply no information at all that is uniquely assigned to a ticket.

The session key that is disclosed is used not only by the ticket-granting-ticket but also by the content tickets as well. Newcombe, ¶¶ 0065, 72. Similarly, the information regarding the user (i.e. account and IP addresses) and life-time parameters all appear in other tickets. *Id.* at ¶ 0072. Finally, the timestamp could hardly be considered "a secret," as one of ordinary skill in the art would understand that term. However, even if it is, Newcombe discloses that the content tickets also include the timestamps. *Id.* ("[C]ontent [S]erver may be configured to perform substantially the same mechanisms to authenticate the client, as described . . . for [the] [Ticket Granting Server]").

Thus, even if a ticket is "similar to a token," as alleged, Newcombe provides no disclosure or suggestion that a secret is uniquely assigned to a "ticket." The Office Action does not assert that the other cited reference discloses these features, nor is there any other suggestion in the record that the other reference remedies these deficiencies of Newcombe.

Whether considered alone or in combination, the references as applied by the Office Action fail to support a *prima facie* case of obviousness with respect to claims 1, 2 and 6. The rejection of dependent claims 3-5 and 7-9 is similarly unsupported by the Office Action, and these claims are allowable for at least the same reasons as the independent claims. For at least this reason, the rejection of claims 1-9 should be withdrawn.

Claims 2-11: The Final Office Action Fails to Show that the Cited References Disclose or Suggest that if the Calculated One Time Password Does Not Correspond to the Received One Time Password, then Incrementing the Count and Recalculating the One Time Password.

Claim 2 recites a method for authenticating a request for access to a resource, comprising, in relevant part:

> if the calculated One Time Password does not correspond to the received One Time Password, then incrementing the value of the count at the authentication server and recalculating the One Time Password based upon the incremented count and the secret, and comparing the recalculated One Time Password with the received One Time Password;

Independent claim 6 recites similar features. The Office Action admits that Matyas and Newcombe do not explicitly teach incrementing the count and/or recalculating as recited. Final Office Action, p. 10. However, the Final Office Action asserts that "Newcombe teaches a window of acceptable values for time with which recalculation can occur and authenticate the client." *Id.* The Office Action alleges that a predictable result of the combination of Matyas and Newcombe is to "substitute the count value for the time value, perform the incrementing of the count and recalculate to determine if the count was acceptable." *Id.* Appellants respectfully disagree.

The window of acceptable values for a timestamp in Newcombe is not a window within which recalculation can occur as the Office Action alleges. Newcombe discloses a method where the timestamp is extracted from a modified authenticator (the modified authenticator is encoded by the User and is a combination of the local and remote IP addresses and the timestamp). Newcombe, Fig. 8; Fig. 9; ¶¶ 0057, 0059. The server then determines if the timestamp falls within a predetermined range - if it does, the user is authenticated; if it does not, the user is not authenticated. *Id.* at ¶¶ 0092, 97. Notably, there is no recalculation of the modified authenticator or any other calculation if the timestamp falls outside the range. Thus, even assuming, *in arguendo*, that a count could be substituted into Newcombe for the timestamp, the count would simply be extracted from the modified authenticator and then checked to see if it was within a range of count values stored on the server.

The proposed modification of Newcombe by the count in Matyas does not disclose that if the calculated One Time Password does not correspond to the received One Time Password, then incrementing the count and recalculating the One Time Password. Therefore, the Office Action fails to establish a *prima facie* case of obviousness and the rejection of claims 2 and 6 should be withdrawn. The rejection of dependent claims 3-5 and 7-11 is similarly unsupported by the Office Action, and these claims are allowable for at least the same reasons as the independent claims. For at least this reason, the rejection of claims 2-11 should be reversed.

The Final Office Action further alleges that these features "are merely reciting optional language," and therefore "are not-limiting and are not entitled to patentable weight." This is incorrect. As noted in MPEP §§ 2106, Part IIC and 2111.04, whether or not a claim term limits

the scope of the claim is fact-dependent, and is determined according to, for example, the grammar and intended meaning of the terms in the claim. The "if" clauses identified by the Final Office Action cannot be considered in a vacuum; rather, they must be read in the context of the claims. For example, claim 2 recites comparing a calculated One Time Password (OTP) to a received OTP. Claim 2 further recites two functions, one of which is performed if the two OTPs match, the other if they do not. Notably, for any two OTPs, there is no third option – either they match, or they do not. Thus, the three features (comparing the OTPs and performing one function or another) together serve to limit the scope of the claim. A similar argument applies to independent claim 6. For at least these reasons, the Final Office Action's assertion that these features are not entitled to patentable weight is incorrect.

Claims 2-11: The Office Action Fails to Show that the Cited References Disclose or Suggest Retrieving the Value of a Count that Corresponds to a Token Based Upon a Serial Number or a User Name.

Claim 2 recites, in relevant part:

> A method for authenticating a request for access to a resource, comprising:
>
> retrieving by the authentication server the value of a count that corresponds to the token based upon the serial number;
>
> calculating by the authentication server the value of a One Time Password based upon retrieved values of the count and the secret corresponding to the token;

Claim 6 recites similar features. The Office Action alleges that "Matyas discloses retrieving a count." Final Office Action, p. 9. However, the Office Action fails to show where Matyas discloses that the value of the count that is retrieved corresponds to a token based upon a serial number. Similarly, the Office Action fails to show that Matyas discloses retrieving the value of a count that corresponds to a token based upon a username as recited in independent claim 6.

There does not seem to be any disclosure in either reference that could be reasonably interpreted to cover these claim features. Indeed, the section of Matyas relied on by the Office Action to make this rejection merely describes various key-specific information:

> Key-specific information 202 comprises information that changes for each invocation of hash function 430. As shown in FIG. 3, this information 202 may comprise an algorithm ID 206, which identifies the cryptographic algorithm in which the generated keys are used, together with the count 420. (For simplicity, only the count is shown in FIG. 4.) Count 420 is incremented for each successive hash with the same input values Zl and Z2, and is reset whenever Zl or Z2 or the algorithm ID changes. The optional other information 204 may include public information contributed by the parties 102 and 104, public information mutually known to both parties, mutually known private information (such as an authentication key communicated over a separate channel or Zl ‖ Z2), or the like.

Matyas, Col. 5, lines 46-59. There is simply no suggestion in this disclosure that the count value corresponds to a token based on a serial number or a user name.

The Final Office attempts to rebut this argument by stating that it is "only directed at the Matyas reference when a combination of Newcombe was provided," and that "one cannot show nonobviousness by attacking references individually." Final Office Action, p. 6. Presumably, the Final Office Action refers to a cite to Newcombe's disclosure of an IP address and a personal identification number (PIN) (*see* Final Office Action, p. 9). Even if the IP address and PIN are properly considered to disclose a serial number or a username, which Appellants do not concede, the Final Office Action fails to make any logical connection between these items in Newcombe and the "count" retrieved by Matyas. There is no description of why one of skill in the art would link Matyas' hash count with Newcombe's IP address and/or PIN, or any other analysis to support the alleged combination and correspondence of features with the claim terms. Thus, as applied by the Final Office Action, the combination of references does not teach a count that corresponds to a token based upon a serial number or a username as recited in independent claims 2 and 6, respectively.

For at least these reasons, the Final Office Action fails to establish a prima facie case of obviousness with regards to claims 2 and 6. The rejection of dependent claims 3-5 and 7-11 is similarly unsupported by the Office Action, and these claims are allowable for at least the same reasons as the independent claims. Appellants respectfully submit that the rejection of claims 2-11 should be reversed.

8. CONCLUSION

For these reasons, it is respectfully submitted that the rejection should be reversed.

Respectfully submitted,

/ASKamlay/
Aaron S Kamlay
Reg. No. 58,813

DATE: December 13, 2010

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 202-481-9900
Fax: 202-481-3972

63044284 v1

9. CLAIMS APPENDIX

1. A method for calculating a One Time Password, comprising:

concatenating, by a computer, a secret with a count, where the secret is uniquely assigned to a token and is shared between the token and an authentication server, and the count is a number that increases monotonically at the token with the number of One Time Passwords generated by the token and increases monotonically at the authentication server with each calculation by the authentication server of a One Time Password;

calculating, by a computer, a hash based upon the concatenated secret and count; and

truncating the result of the hash to obtain a One Time Password.

2. A method for authenticating a request for access to a resource, comprising:

receiving by an authentication server a request for authentication that includes a serial number that is uniquely associated with a token, a personal identification number associated with a user and a One Time Password generated by a token, wherein the One Time Password is based upon the value of a count at the token and a secret shared between the token and the authentication server;

retrieving by the authentication server the value of a count that corresponds to the token based upon the serial number;

retrieving by the authentication server the secret that corresponds to the token based upon the serial number;

calculating by the authentication server the value of a One Time Password based upon retrieved values of the count and the secret corresponding to the token;

comparing the calculated One Time Password with the received One Time Password; and

if the calculated One Time Password corresponds to the received One Time Password, the request is determined to be authenticated;

if the calculated One Time Password does not correspond to the received One Time Password, then incrementing the value of the count at the authentication server and recalculating the One Time Password based upon the incremented count and the secret, and comparing the recalculated One Time Password with the received One Time Password;

if the recalculated One Time Password does not correspond to the received One Time Password, then repeating to increment the count and to recalculate the One Time Password until the recalculated One Time Password corresponds to the received One Time Password.

3. The method of claim 2, wherein the hash function is SHA-l.

4. The method of claim 2, wherein the secret is a symmetric cryptographic key.

5. The method of claim 2, wherein incrementing the count and recalculating the One Time Password is repeated a predetermined number of times, and if the recalculated One Time Password does not correspond to the received One Time Password by the end of the predetermined number of times, the request is determined to be not authenticated.

6. A method for authenticating a request for access to a resource, comprising:

receiving by an authentication server a request for authentication that includes a username that is uniquely associated with a user, a personal identification number associated with a user and a One Time Password generated at a token, wherein the One Time Password is based upon the value of a count at the token and a secret shared between the token and the authentication server;

retrieving by the authentication server the value of a count that corresponds to the token based upon the username;

retrieving by the authentication server the secret that corresponds to the token based upon the username;

calculating by the authentication server the value of a One Time Password based upon retrieved values of the count and the secret corresponding to the token;

comparing the calculated One Time Password with the received One Time Password; and

if the calculated One Time Password corresponds to the received One Time Password, the request is determined to be authenticated;

if the calculated One Time Password does not correspond to the received One Time Password, then incrementing the value of the count at the authentication server and recalculating the One Time Password based upon the incremented count and the secret, and comparing the recalculated One Time Password with the received One Time Password;

if the recalculated One Time Password does not correspond to the received One Time Password, then repeating to increment the count and to recalculate the One Time Password until the recalculated One Time Password corresponds to the received One Time Password.

7. The method of claim 6, wherein the hash function is SHA-l.

8. The method of claim 6, wherein the secret is a symmetric cryptographic key.

9. The method of claim 6, wherein incrementing the count and recalculating the One Time Password is repeated a predetermined number of times, and if the recalculated One Time Password does not correspond to the received One Time Password by the end of the predetermined number of times, the request is determined to be not authenticated.

10. The method of claim 2, wherein the secret is uniquely assigned to the token.

11. The method of claim 6, wherein the secret is uniquely assigned to the token.

10. EVIDENCE APPENDIX

None.

11. RELATED PROCEEDINGS APPENDIX

None.